Testimony Of

Drew Bagley
Vice President & Counsel for Privacy and Cyber Policy
CrowdStrike

Before

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"

March 23, 2023

Chairman Garbarino, Ranking Member Swalwell, members of the subcommittee, thank you for the opportunity to testify today. We are at a pivotal moment in the cybersecurity challenges posed to our country. Today, nation states, criminal enterprises, and hacktivist groups alike can leverage sophisticated means to exploit unsophisticated vulnerabilities to conduct espionage, breach privacy, and wreak havoc on critical infrastructure, government systems, and businesses throughout the country. We are at a point where the stakes of defensive stagnation pose increasing risks in the face of threat actors' innovation. This is why it's so important to continually evolve in how we prevent, detect, and respond to cyber attacks.

Throughout my career, I have seen firsthand the challenges and opportunities of improving American cybersecurity from my work in the private sector, government, and academia. For nearly a decade, at CrowdStrike, a leading cybersecurity company, I have had a front row seat to cybersecurity innovation while building our privacy and public policy programs and advising customers around the globe. Prior to that I worked at the intersection of law and technology in the FBI's Office of the General Counsel. I previously taught at universities in the US and Europe, and currently serve as an adjunct professor in American University's cybersecurity policy program. I have been asked to speak here today from a stakeholder perspective. Accordingly, my testimony is informed not only from my experience but also by my continued engagement with government agencies through formal and informal advisory roles, including as a member of CISA's Joint Cyber Defense Collaborative (JCDC).

At CrowdStrike, we have a unique vantage point on cybersecurity threats and the innovation necessary to stop them. We not only protect 15 of the largest 20 banks in the US but also provide our cybersecurity technology and services to thousands of small and medium sized businesses. This means that it is not only possible for small organizations to leverage the same cybersecurity technologies as complex multinational enterprises but that it is becoming more common.

Increasingly, fundamental aspects of cybersecurity program design are applicable everywhere–including for the ongoing transformation in U.S. federal cybersecurity.

CrowdStrike works with CISA in a variety of ways across key programs and activities. We were one of the original plank holders of JCDC and remain active members to this day. We provide cyber threat intelligence and cybersecurity technology offerings to CISA that help it defend not only its own networks but those of some other government departments and agencies as well. Lastly, we are a consumer of CISA's advisories and a key technology provider for its other stakeholder groups, like critical infrastructure entities.

Key Developments

This hearing is timely for three key reasons. First, over the past couple of years CISA has reached its stride across a number of operational and planning functions (described in more detail below). Second, major transitions are taking place in federal cybersecurity overall, with an emphasis on security program modernization and Zero Trust Architecture. CISA is a key actor and implementer in these areas. Third, geopolitical conditions have yielded a worsening cyber threat environment overall. Russia's war in Ukraine and heightened competition with China are just two of several active examples where risks are mounting.[1]

Now is an impactful time to review the state of cybersecurity overall and evaluate CISA's considerable progress and contributions.[2] As DHS and CISA leadership and Members of this Committee prepare jointly to realize the vision of *CISA 2025,*[3] we can identify fruitful areas for continued development, alignment, and investment, where appropriate.

The State of Cybersecurity

Cybersecurity outcomes vary substantially across different sectors. Different sectors face different threats, have different constraints and capacities, and have different tolerances to risk or disruptions. To this end, I'd like to survey the state of cybersecurity across a few key CISA partner segments.

Federal Civilian Executive Branch (FCEB). Going back 20 years, Federal government agencies often had considerable cybersecurity strengths relative to their private sector counterparts. However, as time went on and cyber attacks increasingly occurred without the use of malware, parts of the private sector met and exceeded FCEB cybersecurity performance by adjusting to new realities. In some instances, government IT standards and controls failed to evolve at the rapid pace of innovation within the commercial IT and cybersecurity space. Large Federal Cybersecurity

[1] *See Adam Meyers, Testimony on Securing Critical Infrastructure Against Russian Cyber Threats*, House Homeland Security Committee (March 30, 2022) (How Russia-nexus adversaries use cyberattacks and recommendations for U.S. readiness), https://docs.house.gov/meetings/HM/HM00/20220405/114553/HHRG-117-HM00-Wstate-MeyersA-20220405.pdf. [2] *See CISA*

Strategic Plan 2023-2025, CISA (September 2022), https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf.
[3] *See CISA 2025 Overview,* Committee on Homeland Security, House of Representatives (October 13, 2022), https://homeland.house.gov/cisa-2025/.

programs (e.g., National Cybersecurity Protection System (NCPS) or EINSTEIN, and the Continuous Diagnostics and Mitigation Program (CDM)) set ambitious goals aimed to standardize and scale approaches to government cybersecurity, but even with considerable investment over the years, that aim remains unmet.

Over the past several years, however, the Federal cybersecurity community has made some significant strides. Recent developments are trending positively with the embrace of key cybersecurity concepts like centralized visibility of IT infrastructure to detect and respond to incidents. Significantly, E.O. 14028 on *Improving the Nation's Cybersecurity*[4] mandated the use across the FCEB of key best practices, like enhanced logging, as well as now-baseline technical solutions like Endpoint Detection and Response (EDR). The release of the Office of Management and Budget's *Federal Zero Trust Strategy*[5]in January 2022 was another key decision enforcing the use of sound approaches, like increased adoption of cloud-based technologies, credential management practices,[6] and defensible IT architectures. Even as implementation continues, these initial efforts are yielding positive results.

CISA plays an essential role in strengthening FCEB cybersecurity. As recently as a couple of years ago, CISA had just a few programs (e.g., NCPS, CDM, Trusted Internet Connections (TIC)) and a few authorities (e.g., Emergency Directives, Binding Operational Directives[7]) to meet this mandate. But the Solarium Commission's recommendation as enacted by Congress to formally elevate CISA to become the operational CISO of the FCEB, including by providing government-wide, proactive cyber threat hunting capabilities, considerably strengthened CISA's toolkit. Further, actions taken by CISA to implement E.O. 14028, particularly with regard to the EDR program, are helping to realize this vision.

The stakes are high. The FCEB continues to be a key target of threat actors that seek to do harm to the United States. Friends and allies continue to look to the U.S. Government as a model for how to organize their own government cybersecurity efforts. And importantly, the government must lead by example on cybersecurity. CISA's efforts to strengthen security across the other entities (e.g., critical infrastructure or state and local governments) will lack credibility if the FCEB is poorly secured.

Large Enterprises. On balance, the most sophisticated large enterprises in the U.S. have seen stronger cybersecurity outcomes in recent years, even as threats evolve and multiply. Over the past year, we've observed an increase in vulnerability reuse and increased reliance on access brokers to facilitate initial infiltration into target organizations. We've also witnessed increased targeting of–and mounting costs from–breaches of legacy infrastructure.[8] Supply chain attacks, which can be

[4] *See Executive Order on Improving the Nation's Cybersecurity,* The White House (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[5] *See M-22-09 Memorandum for the Heads of Executive Departments and Agencies,* Executive Office of the President, Office of

Management and Budget (January 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf. [6] *See 7 TYPES OF IDENTITY-BASED ATTACKS,* CrowdStrike (January 10, 2023), https://www.crowdstrike.com/cybersecurity-101/identity-security/identity-based-attacks/.
[7] *See Cybersecurity Directives,* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/directives.
[8] *See 2023 Global Threat Report,* CrowdStrike (2023). https://www.crowdstrike.com/global-threat-report/.

targeted but also used to breach many dependent organizations in a single campaign, remain a key concern.

Some large commercial enterprises have greater flexibility and stronger security budgets than other entities, and thus serve as an important proving ground for new technologies, practices, and architectures. From this, recent innovations like Zero Trust and cloud-native EDR have become today's cybersecurity essentials. In the near future, we should expect more attention from other sectors on emerging enterprise security concepts like Extended Detection and Response (XDR), identity threat protection,[9] as well as continued adoption of managed security services (discussed in more detail below).

Small- and Medium-sized Businesses (SMB). These entities include everything from the family-owned corner store in each of our communities to startups creating new technologies that could change the world. These companies operate off of very different templates but nevertheless share two key features. First, resources are scarce. Second, a multi-day business disruption might well destroy the company. Resource scarcity means there's no place for complex cyber defenses, and few if any 'spare cycles' for participation in demanding or time-consuming information sharing initiatives. Sensitivity to disruption means these organizations are particularly vulnerable to ransomware and "lock-and-leak" attacks.

Among the most positive developments in this space in recent years is the growing affordability and accessibility of managed security services, as well as managed threat hunting services. Organizations increasingly look to professional providers to manage the overwhelming majority of defense actions–under tight service level agreements–24 hours a day, 7 days a week, 365 days a year.

State, Local, Tribal, and Territorial (SLTT) Entities. Over the past few years, SLTT entities have faced a withering threat environment, most notably from criminal ransomware actors. Materially all SLTT entities face budgetary and personnel constraints, and rely upon critical legacy applications and IT infrastructure. Nevertheless, over that same time horizon, cybersecurity outcomes within the sector have diverged significantly. As Members of this Committee know well, many SLTT organizations faced severe incidents and events, and in some instances citizens suffered disruption of key services.

Counterintuitively perhaps, over this timeframe the most forward-leaning states and cities were meaningfully further ahead than most of the FCEB in centralizing and modernizing defenses. This was generally achieved through a key service provider–typically a Department of Technology–implementing and managing transformative technologies like EDR and other important security concepts and practices. In addition to leveraging a centralized provider, these states often had no inflexible security program that acted as a barrier to experimentation and technology

[9] *See Andrew Harris, CrowdStrike Falcon Identity Threat Protection Added to GovCloud-1 to Help Meet Government Mandates for Identity Security and Zero Trust,* CrowdStrike (June 1, 2022), https://www.crowdstrike.com/blog/how-falcon-identity-threat-protection-helps-meet-identity-security-government-mandates/.

adoption. In addition, community-oriented support efforts, such as those led by the Center for Internet Security, have been a key part of stronger defenses.

The State and Local Cybersecurity Improvement Act, which passed into law in the Infrastructure Investment and Jobs Act of 2021 was a positive step in ensuring state and local governments have the funding needed to centralize and modernize cyber defenses. We appreciate former subcommittee Chairwoman Clarke, Chairman Garbarino, and other members of the committee for their leadership on this important issue.

Critical Infrastructure. Most critical infrastructure owners and operators face the same set of hardships outlined above: severe threat environment, personnel and budget constraints, and legacy applications and IT infrastructure. But they have the added challenges of complex Operational Technology (OT) that in some instances is obsolete and/or esoteric. In addition to these conditions there is increased interest from policymakers in regulatory measures designed to enhance cybersecurity.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law in March 2022, which strengthens reporting obligations for critical infrastructure players, is the most meaningful step to date.[10] CIRCIA's authors–notably Members and key staff on this Committee–recognized these risks and included two key provisions. The first is a Cyber Incident Reporting Harmonization Council that should reconcile duplicative or conflicting regulations. The second is a generous timeline for CISA to articulate particulars (like thresholds) in a clear and straightforward manner. CISA has solicited stakeholder feedback to those ends, to which we, and many others in the community, were happy to contribute ideas and suggestions.[11]

International. Although somewhat beyond the scope of this hearing, we should take a moment to reflect on international cybersecurity. U.S. allies' public sector organizations, laws, and policy debates tend to reflect somewhat developments here in Washington. This is an incredible leadership opportunity. Efforts like the International Counter Ransomware Initiative[12] serve as a good example for how to use this influence to strengthen the cybersecurity ecosystem globally. Across relevant areas of law and policy, we should embrace interoperable approaches that simplify collaboration between governments, NGOs, and industry players. In addition, the U.S. should be receptive to areas where other countries have identified helpful policies. These include, for example, policies that support the startup ecosystem, and national privacy laws that simplify data protection and the cross-border data flows integral for modern cybersecurity.[13]

[10] *See Public Law 117 - 103, Division Y, Cyber Incident Reporting for Critical Infrastructure Act - Consolidated Appropriations Act, 117th Congress (March 15,* 2022). https://www.congress.gov/bill/117th-congress/house-bill/2471/text. [11] *See CrowdStrike Response*

to RFI on Cyber Incident Reporting for Critical Infrastructure Act (November 14, 2022), https://www.crowdstrike.com/wp-content/uploads/2023/02/RFI-Incident-Reporting-for-Critical-Infrastructure-Act-of-2022.pdf. [12] *See International Counter Ransomware Initiative 2022 Joint Statement,* The White House (November 1, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.
[13] *See Drew Bagley, Data Protection Day 2023: Misaligned Policy Priorities Complicate Data Protection Compliance,* CrowdStrike (January 27, 2023), https://www.crowdstrike.com/blog/data-protection-day-2023-misaligned-policy-priorities-complicate-data-protection-compliance.

Public-Private Collaboration

The Joint Cyber Defense Collaborative (JCDC). Information sharing in the cybersecurity space is a complex topic and longstanding policy priority. For two decades, various information sharing efforts–narrow and broad; informal, quasi-official, and official; *ad hoc* and enduring–have arisen from a desire within the cybersecurity community to do more. While the Cybersecurity Act of 2015 sought to address this problem head on,[14] structural impediments to comprehensive sharing and collaboration remain.[15] And as a practical matter, we are unlikely to identify a "silver bullet" solution to a problem with this many complexities. However, the formation of JCDC in August 2021 was a key development in promoting sharing and collaboration. In the time since, JCDC has created a platform for key players in industry and government to voluntarily work toward common goals.

While we would generally defer to CISA Leadership to describe key outcomes, we can say that CrowdStrike values the partnership opportunity. We continue to invest time and expertise in the JCDC community, and we look forward to continued, shared efforts to promote better cybersecurity.

As JCDC matures, we believe the effort can continue to improve. Two suggestions:

- **Consider approaches that stratify or segment membership to maintain trust**. As the group expands, JCDC leadership should account for the possibility that some members may become less willing to share details about sensitive issues. JCDC has addressed this concern by maintaining clear direct channels of communication with participants, and creating ad hoc working groups with a subset of members. These are important measures, but additional subgroup governance may help promote more active and applied sharing. Articulating long-term aims for membership composition may also be of value.
- **Strengthen *administrative* Customer Relationship Management (CRM) practices**. This would ensure consistent notification of participant stakeholders about upcoming opportunities, events, engagements, etc. A designated partner "JCDC relationship owner" should be able to flexibly add or remove corporate participants from various JCDC workstreams to facilitate participation from particular personas (e.g, according to function, experience, protocol, etc.).

To their credit, JCDC leadership and staff have been proactive about seeking feedback from participants. We have provided suggestions along these lines to them directly and believe it is taken seriously. Like any "startup," we anticipate continued iteration as the group matures into its full potential.

Ecosystem. CISA contributes to the cybersecurity ecosystem in a variety of other ways. Support to key partners in the SLTT community; advice and tools for enhancing infrastructure, Industrial

[14] *See Public Law 113-113, Division N, Cybersecurity Act of 2015.* 114th Congress (December 18, 2015), https://www.congress.gov/bill/114th-congress/house-bill/2029/text
[15] *See George Kurtz, Questions for the Record - Hearing on the Hack of U.S. Networks by a Foreign Adversary,* Senate Select Committee on Intelligence (February 23, 2021) (How the private sector has promoted practical information sharing),https://www.intelligence.senate.gov/sites/default/files/documents/qfr-gkurtz-022321.pdf.

Control Systems (ICS), and OT security; alerts and notifications for IT security, particularly around emerging vulnerabilities; and leadership on workforce topics all contribute to better cybersecurity outcomes. Each of these issue areas is complex and requires specific expertise. CISA's contributions in this realm continue to mature and become more valuable over time.

There remains a gap in cybersecurity performance between the "haves" and the "have-nots," which threat actors continue to exploit and which CISA cannot solve alone. To this end, we are pleased to see reference in the new National Cybersecurity Strategy to shifting the burden for cybersecurity to those best positioned to mitigate risks. This includes, where appropriate, holding platform providers accountable for the security of their products.[16] As a community, we should no longer tolerate certain software vendors externalizing the costs of–or worse, nakedly monetizing–insecure software applications.[17] While this policy concept must be made more concrete, a reasonable first step is ensuring that we're not rewarding vendors that cause harm. To this end, the government can lead by example by using its own procurement power to shape market dynamics. This is clearly a productive area for continued congressional oversight.

Recommendations

1. **The entire field must become more responsive in adapting to lessons learned**. Unfortunately, cyberattacks with the potential for systemic implications take place with increasing regularity. However, organizations are uneven in adopting key lessons, from new security controls and mitigations to more secure architectures. From our vantage point, key lessons of recent breaches include:

- Use managed security services where practical to augment internal security staff and attain responsive and comprehensive security coverage.
- Adopt cloud-based IT systems and where possible, leverage cloud-based security tools to achieve scalability and speed.
- Employ Zero Trust Architecture, with emphasis on identity threat protection, to defend an increasingly diffuse IT infrastructure and radically reduce lateral movement during breach attempts, bringing us closer to cyber and mission resiliency.

2. **We must approach regulation deliberately and harmonize to the greatest extent possible.** Even as CIRCIA advances through rulemaking, independent regulators are pursuing new obligations[18] and the National Cybersecurity Strategy foreshadows additional actions at the

sector-level.[19] Each of these measures is well-intended, but taking place simultaneously and with different stakeholders. At best, they will close longstanding gaps and strengthen national resilience.

[16] *See National Cybersecurity Strategy, page 20.* The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [17] For one example of a persistent security issue, see *George Kurtz, Testimony on Cybersecurity and Supply Chain Threats,* Senate Select Committee on Intelligence (February 23, 2021) (Extended discussion on emerging cybersecurity controls and practices), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf. p. 5.
[18] *See TSA issues new cybersecurity requirements for airport and aircraft operators,* Transportation Security Administration (March 7, 2023), https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft [19] Even prior to CIRCIA and recent efforts, data breach victims commonly faced more than 50 different reporting requirements in the U.S. alone, with additional international obligations in many cases.

At worst, they risk yielding burdensome, distracting, and costly compliance obligations without additional security gains. Optimizing for the former is among the most important challenges the cybersecurity policy community faces at this time. Our hope is that continued collaboration between potential regulators and/or muscular harmonization efforts will help avert worse outcomes. The best advice we can offer is:

- Be deliberate about advancing new requirements;
- Provide formal commenting periods for stakeholders to contribute views; ● Use principles-based requirements rather than burdensome and inflexible compliance-based approaches;
- Include provisions to regularly review and if necessary modify, update, or deprecate requirements or controls based on developments in the threat environment or technology ecosystem;
- The DHS Cyber Incident Reporting Council established under CIRCIA should operate with vigor, and work to clearly identify and reduce duplicative reporting; and
- Set the goal of all federal agencies showcasing cybersecurity best practices with a particular emphasis on those that regulate cybersecurity "walking the walk."

3. **As a community, we should focus more attention on national incident response capacity.** JCDC should continue coordinating and developing community response plans and CISA should weigh potential JCDC contributions for the purposes of forthcoming revisions to the National Cyber Incident Response Plan (NCIRP).[20]If the Russian threat actors responsible for the major supply chain attack or the Chinese threat actors responsible for the Microsoft Exchange hacking campaign in 2021 had deployed ransomware or pseudo-ransomware at scale, large segments of the American economy would have been paralyzed. A CISA-administered program to retain outside providers for emergency incident response to attacks at entities of systemic importance could be of tremendous value in a future contingency.[21] This could mitigate crippling impacts and ensure CISA had the ability to orchestrate response activities and maintain insight into findings in real time.

4. **We must empower defenders with cutting edge cyber-defense capabilities.** Defenders with leading solutions are energized with radically improved morale. Too often, defenders are hobbled with inefficient and ineffective technologies. When these inevitably fail, they begin to feel like little

more than a punching bag for adversaries, and that their best efforts are for naught. But when people are empowered, they can see their impact each day and can remain focused on the importance of their mission. To the extent that this Committee can promote access to better tools, that will absolutely strengthen cybersecurity outcomes. For the FCEB, this means the full adoption of technologies mandated in E.O. 14028 like EDR and, ultimately, better access to managed security services to augment staff. To highlight another opportunity, we believe it's time to have a more

[20] *See National Cybersecurity Strategy, page 12.* The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. [21] *See Robert Sheldon,Testimony on Protecting American Innovation, Senate Select Committee on Intelligence (September 21, 2022),* https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf.

serious conversation as a community about using tax mechanisms to speed adoption of key technologies in the SMB space.[22]

5. **The community must attract and retain top cybersecurity talent.** The level of talent in our field–across industry and government–is deeply inspiring. Based on our experience, the central motivator for people in the field is a sense of mission. A key challenge we have as a community is overburdened staff leading to burnout, a concern that underpins some of my previous comments on leveraging managed services and mitigating time-consuming and ineffective compliance obligations. Further, aligning roles to each organization's key missions–and in the case of government authorities–helps people recognize the uniqueness of their contributions. A second challenge is expanding recruitment efforts to grow additional talent. To this end, I was pleased to announce during my participation at a White House Summit last month that CrowdStrike would soon launch an emerging leaders program focused on diverse candidates.[23] We must continue efforts to fuel the cybersecurity talent pipeline.

CISA's evolution is the culmination of non-partisan efforts under four consecutive presidential administrations, and CISA has received numerous new key authorities and increases in funding over the past several years. Ultimately, in each passing year it is important to ask whether the US government is better able to prevent, detect and respond to cyber attacks. Accordingly, I am pleased to see this committee has identified key oversight areas in the CISA 2025 initiative to put CISA on track to fully implement those authorities and fulfill the mission Congress has entrusted it with. CrowdStrike looks forward to continuing and building upon its trusted relationship with CISA, and playing our part in empowering it to effectively carry out its mission.

Thank you for the opportunity to appear in front of you today, and I look forward to your questions.

###

[22] *See Robert Sheldon, Testimony on Protecting American Innovation,* Senate Select Committee on Intelligence (September 21, 2022), https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf.

[23] *See Readout: Office of National Cyber Director Hosts Roundtable on "The State of Cybersecurity in the Black Community"* The White House Briefing Room (February 28, 2023), https://www.whitehouse.gov/oncd/briefing-room/2023/02/28/readout-office-of-national-cyber-director-hosts-roundtable-onthe-state-of-cybersecurity-in-the-black-community/.

Testimony of Heather Hogsett

Senior Vice President, Technology and Risk Strategy for BITS, the Technology Policy Division of the Bank Policy Institute

Before the U.S. House Subcommittee on Cybersecurity and Infrastructure Protection
"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"

March 23, 2023

Chairman Garbarino, Ranking Member Swalwell and Honorable Members of the Subcommittee, thank you for inviting me to testify. I am Heather Hogsett, Senior Vice President of Technology and Risk Strategy for BITS, the technology policy division of the Bank Policy Institute (BPI).

BPI is a nonpartisan policy, research and advocacy organization representing the nation's leading banks. BPI members include universal banks, regional banks and major foreign banks doing business in the United States. BITS, our technology policy division, works with our member banks as well as insurance, card companies and market utilities on cyber risk management and critical infrastructure protection, fraud reduction, regulation and innovation.

I also serve as Co-Chair of the Financial Services Sector Coordinating Council (FSSCC) Policy Committee. The FSSCC coordinates across the financial sector to enhance security and resiliency and to collaborate with government partners such as the U.S. Treasury and the Cybersecurity and Infrastructure Security Agency (CISA), as well as financial regulatory agencies.

Financial Institutions and Cybersecurity

Banks and other financial institutions are increasingly under cyber-attack by foreign nations and criminal groups seeking to disrupt the financial system and undermine the functioning of the U.S. economy. The financial sector takes these risks seriously and has a long history of working across industry and with government partners to address and manage these risks.

As one of 16 critical infrastructure sectors, the financial industry formed and actively participates in the FSSCC[1]and the Financial Services Information Sharing and Analysis Center (FS-ISAC)[2] — both of which have served as leading examples other critical infrastructure sectors have sought to replicate. We also lead cybersecurity and operational resilience collaboration through public-private partnerships with our Sector Risk Management Agency (SRMA) — the U.S. Department of the Treasury — the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and importantly with our regulators.

A major part of these industry efforts is focused on in-depth information sharing to accelerate and amplify public-private cooperation. During the nearly two decades of work, we have established exercise programs through the FSSCC and FS-ISAC that have covered a wide range of possible events such as destructive malware, an outage at a large service provider, or a pandemic and addressed

[1] https://fsscc.org/
[2] https://www.fsisac.com/

managing public confidence during a crisis. More than 40 such exercises have been held to date and have included participants from across the industry, third parties, regulators, the U.S. Treasury Department, DHS/CISA and law enforcement agencies.

In addition to Treasury and CISA, we also work closely with financial regulators to address cybersecurity, third-party and supply chain risks and promote operational resilience across the sector. This work occurs with individual firms, through trade associations such as BPI, and via joint efforts between the FSSCC and its government counterpart the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by Treasury and includes 17 federal and state regulators.[3]

Experiences with CISA

Since its establishment in 2018 as an operational component of DHS, CISA has taken on an increasingly important role protecting federal civilian agencies and supporting security and resilience across critical infrastructure sectors. Following the important coordination role CISA filled during the COVID-19 pandemic to keep critical infrastructure working for America, there have been notable improvements in faster declassification and sharing of threat information, including a significant increase in publications, alerts and joint advisories with other government agencies such as the FBI and National Security Agency (NSA). These publications have become more frequent, timely and relevant and included recommended mitigation measures to help critical infrastructure entities better protect themselves, particularly midsize and smaller entities where the assistance is needed most. For example, CISA's recommended mitigations and tool kits to help entities protect themselves during the response to Solar Winds, Log4j and the ransomware attack against Colonial Pipeline were welcome for their timeliness and actionable nature. By creating a centralized repository for this information CISA has also made it easier for companies to quickly find and access relevant information and resources.

Its efforts to help raise awareness and promote baseline cybersecurity practices across all critical infrastructure sectors have been a welcome focus that will help reduce risk and improve national resilience. CISA also deserves credit for fostering collaboration and coordination across government entities including the banking industry and other critical infrastructure. Its work to date has built the foundation for trusted relationships and very importantly created resources to support those sectors that are resource constrained and in the earlier stages of building their cyber risk management programs.

The preparation and response to the Russian invasion of Ukraine highlight a number of these accomplishments. As tensions rose and the U.S. prepared for Russian aggression and the potential for retaliatory attacks, CISA's senior leadership, along with senior leaders at Treasury, DHS and the FBI, was in regular communications with financial institutions and organizations like the FSSCC, FS-ISAC and the Analysis and Resilience Center for Systemic Risk (ARC). CISA created the "Shields Up" campaign to raise awareness and urge critical infrastructure companies to shore up their defenses and actively share suspicious information with the government to provide an early warning of attacks. During this time, CISA created a new bi-directional communication mechanism to provide for near real-time information sharing among trusted partners in both industry and government that had never previously been done. This coordination role was invaluable for our industry and others and provided a streamlined mechanism to exchange threat information and share timely updates to those operating some of the nation's most critical infrastructure.

[3] www.fbiic.gov

Evolving for the Future

Looking ahead, it will be important for CISA to establish a clear path for maturing and scaling its operations, including ensuring these programs and initiatives have stakeholder input and will continue despite future changes in leadership. A number of the efforts to date have been in response to current cyber threats, which was and continues to be important, but CISA is also uniquely positioned to address longer-term strategic planning and cross-sector risk mitigation that will be particularly valuable for mature sectors. As CISA continues to evolve, we encourage a focus on the following areas:

- ***Cyber Incident Reporting and Harmonization – Supporting Response and Recovery*** Last year, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, requiring critical infrastructure companies to report ransomware payments and cyber incidents to CISA. BPI supported this legislation which we believe will help improve national cyber defense by providing CISA and other government agencies with timely and relevant information to assess and analyze cyber threats across sectors, improve the alerts and security services CISA provides and ultimately provide earlier warning of potential attacks so companies can better defend themselves. Under the law, CISA must conduct a rulemaking process, seek input from stakeholders, and develop the necessary systems and processes to collect, analyze and share reported information while ensuring strong data security and protection measures are in place.

  As CISA crafts rules under CIRCIA, it is also required to harmonize the new requirements with existing regulatory reporting to avoid conflicting, duplicative or burdensome requirements. Given the comprehensive set of cybersecurity and incident notification rules[4] that financial institutions already comply with, harmonizing and aligning the new rules will be important to ensure cyber defenders can maintain focus on protecting the firm rather than complying with multiple government reporting requirements.

  This is a significant undertaking that CISA must get right from the outset and will require extensive coordination with critical infrastructure entities, SRMAs, other government agencies and independent regulators. As a critical infrastructure sector that has had mandatory cyber reporting requirements for more than 20 years and has invested significant time and resources into harmonizing and driving toward regulatory convergence, this is a key area of focus. CISA should ensure that definitions, timelines, thresholds and required incident information are aligned with existing requirements and designed to avoid interfering with response and mitigation at an affected firm.

  BPI recommends that CISA build a streamlined reporting system that accomplishes the following: 1) allows an impacted firm to report incident information once and have it shared, as appropriate, with SRMAs, regulators and law enforcement agencies; 2) provides CISA with timely and relevant information useful to assessing trends, improving analysis, and the development of alerts, tools and services that can be provided to critical infrastructure companies; and 3) maintains its role as a trusted channel for information and communications, preserving privacy and confidentiality while supporting the response and recovery of an impacted entity.

[4] https://staging4.bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/

- ***Identification and Prioritization of National Systemic Risks***

  Identifying critical infrastructure assets that are most important to our national security would help prioritize resources and guide public-private collaboration to prevent or mitigate threats and prepare for potential response and recovery needs.

  Financial institutions have existing designations such as the Systemically Important Financial Institution designation that stems from the Dodd-Frank Act of 2010 and requires firms to adopt enhanced measures for security and resilience and includes additional oversight and examination by financial regulators. Many of these firms are also included in the Section 9 process, established by Executive Order 13636 in 2013 and managed by DHS, which recognizes firms where a cyber incident could result in "catastrophic regional or national effects on public health or safety, economic security or national security."

  Similarly, in 2019, CISA created a list of 55 National Critical Functions that are functions "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[5] CISA is in the process of working with SRMAs to decompose or analyze these further. At the same time, CISA is developing a new designation for Systemically Important Entities (SIEs) and was appropriated an increase of $1.9 million for the creation of an SIE Program Office.

  Financial institutions are very supportive of efforts to better identify and prioritize cross-sector risks; however, the current approach appears disjointed and opaque, making it challenging for industry to provide input or information that might be helpful. Past proposals to create an SIE or Systemically Important Critical Infrastructure (SICI) designation would have duplicated existing designations and requirements on financial institutions, diverting resources from defending against threats to regulatory compliance.

  As CISA continues this work, we encourage greater transparency and clarity in the approach, what it intends to accomplish, and how an SIE designation fits with related areas of work such as the Section 9 list, NCFs and sector-specific systemic risk designations such as SIFI. CISA should not only avoid duplication or overlap with other systemic designations and their requirements but also leverage work that has already been done in the more mature critical infrastructure sectors. Financial institutions have worked through the ARC to analyze financial sector systemic risks and are ready to work with CISA to develop a framework for assessing risks and critical dependencies across sectors.

- ***Fostering Cross-Sector Coordination and Operational Collaboration***

  CISA's role as national coordinator for critical infrastructure security puts it in a unique position to support collaboration among more mature sectors and the government to reduce risk and disrupt threats. Since 2017, the financial, energy and communications sectors have conducted joint planning and exercises to address cyber threats that could impact or cascade across the three sectors. CISA supported the creation of the "tri-sector" working group which is a good

example of fostering and enabling collaborative efforts.

[5] https://www.cisa.gov/national-critical-functions

CISA's Joint Cyber Defense Collaborative (JCDC) was helpful in bringing together industry and government partners to improve visibility and communication in response to geopolitical tensions and the Russian invasion of Ukraine. This response-oriented focus, however, has not fulfilled the need for longer-term strategic planning across government agencies and the private sector. As originally authorized by Congress,[6] CISA was charged with creating a Joint Cyber Planning Office (JCPO) to develop plans for cyber defense operations and coordinated actions that public and private sector entities could take to protect, mitigate, or defend against malicious cyber-attacks. To date, we have not seen the JCDC engage in the type of planning directed by Congress but continue to believe this would be beneficial for financial institutions and other more mature sectors.

The recently released National Cybersecurity Strategy recognizes that the private sector has growing visibility into adversary activity and calls for enhancing public-private operational collaboration to disrupt adversaries.[7]Through our relationship with Treasury as our SRMA, we have robust partnership and dialogue. Treasury is establishing a cyber collaboration center to facilitate greater opportunity for firms to exchange classified and unclassified information and facilitate discussion around threat actor activity and vulnerabilities. Other parts of government have created similar centers such as the NSA's Cybersecurity Collaboration Center. Plans to create a cross-sector equivalent or otherwise foster collaboration and exchange among these efforts would be valuable and CISA could play a helpful role.

Sustaining Progress and Building Capabilities

We are at a defining juncture in CISA's development, similar to any startup at this stage, where achieving scale matters. As Congress intended and supported with funding, CISA must refine its focus and apply resources carefully to be successful. Now that CISA has established its presence, developed communications and outreach capabilities, and designed tools and services to improve near-term resilience, it should shift its approach to expand management capabilities, add operational expertise and establish processes that will be the foundation for sustained leadership on immediate tactical response matters as well as longer-term, proactive planning and support that will benefit even the most cyber mature sectors like financial services.

Successful implementation of CIRCIA, including harmonizing its reporting requirements to optimize protection and response and streamline coordination, will serve as a cornerstone for the future of public-private partnerships and should be a top priority. Similarly, developing the means to identify and prioritize the highest risks by sector and across sectors will refine CISA's focus and support more secure and resilient outcomes for the nation.

This is no small task and requires CISA to focus on building organizational consistency and rigor, hiring and retaining experienced staff, and sourcing support from sectors that have well-established security, resilience and, in the financial services case, regulatory standards that can be leveraged.

We are committed to working with CISA to support its continued development and look forward to the

opportunity to engage in future national risk mitigation efforts.

[6] *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*. P.L. 116-283, Sec 1715.
[7] National Cybersecurity Strategy, March 2023, p. 15

Marty Edwards
Deputy CTO OT/IoT, Tenable, Inc.
House Homeland Security Committee
Subcommittee on Cybersecurity and Infrastructure Protection
"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"
March 23, 2023

Introduction

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and members of the Subcommittee, thank you for the opportunity to testify before you today on the Cybersecurity and Infrastructure Security Agency (CISA) and the state of American Cybersecurity.

My name is Marty Edwards and I am the Deputy Chief Technology Officer for Operational Technology (OT) and Internet of Things (IoT) at Tenable, a cybersecurity exposure management company that provides organizations, including the federal government, with an unmatched breadth of visibility and depth of analytics to measure and communicate cybersecurity risk. My expertise is in OT and Industrial Control System (ICS) cybersecurity, and my work with Tenable has focused on furthering government and industry initiatives to improve critical infrastructure security. In collaboration with industry, government and academia, Tenable is raising awareness of the growing security risks impacting critical infrastructure and of the need to take steps to mitigate those risks. I also recently served as the staff lead under Tenable Co-Founder Jack Huffard in the development of the Report on Information Technology (IT)/OT Convergence Report[1]issued by The President's National Security Telecommunications Advisory Committee (NSTAC). Prior to joining Tenable, I worked in industry as an Industrial Control Systems Engineer and as a Program Manager at the U.S. Department of Energy's Idaho National Laboratory focused on cybersecurity. I was the longest-serving Director of the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which is now part of CISA.

About Tenable

Tenable is headquartered in nearby Columbia, Maryland, and has 1,900 employees globally and approximately 43,000 customers worldwide. Tenable is publicly traded on the NASDAQ and is the world's leading provider of vulnerability management capabilities. We believe cybersecurity is foundational to making better and more strategic decisions. Our goal is to eliminate blind spots and help organizations prioritize which actions they can take to most efficiently reduce exposure and loss.

Tenable empowers organizations of all sizes to understand and reduce their cybersecurity risk. For the federal government specifically, Tenable provides the most widely deployed vulnerability management solution, serving just about every department and agency. Our solutions are also broadly used by state and local governments to manage cybersecurity risk.

[1] President's National Security Telecommunications Advisory Committee, "Information Technology and Operational Technology Convergence Report,"
https://www.cisa.gov/sites/default/files/publications/NSTAC%20IT-OT%20Convergence%20Report_508%20Compliant_0.pdf

The Current State of OT/Critical Infrastructure/Federal Cybersecurity

Over the past few years, we have seen a dramatic increase in the frequency of successful cyberattacks against U.S. public- and private-sector organizations and have experienced new threats targeting our critical infrastructure. New ransomware and extortion groups routinely exploit known vulnerabilities to gain access into organizations, with at least 31 new groups discovered from November 2021 to October 2022, resulting in ransomware attacks intensifying, exposing reams of data and accounting for over 35% of data breaches.[2]

In February 2021, a water treatment plant in Oldsmar, Florida, was breached when attackers attempted to poison the water supply.[3]Just months later, a ransomware attack against Colonial Pipeline shut down operations for six days, prompting the President of the United States to issue a state of emergency.[4] Following Russia's invasion of Ukraine last year, and increased threats of malicious activity against the U.S. and our allies, CISA and other law enforcement agencies took swift steps to warn governors, public sector partners and critical infrastructure providers to harden their cyber defenses, including through the "Shields Up" initiative.[5]

Just this month, a breach of D.C. Health Link, the health insurance exchange which serves members of Congress and their staff, resulted in the online exposure of personal data of more than 56,000 customers.[6] While unfortunate, this breach is not surprising as healthcare was the No. 1 sector targeted by ransomware attacks last year with 472 breaches, followed by the public administration sector, which includes governments, towns, and municipalities with 162 breaches.[7]

When it comes to reducing cyber risk, organizations worldwide find themselves restricted by deeply entrenched people, process and technology issues. An orientation toward reactive, incident-focused cybersecurity practices means preventive tasks are often relegated to nothing more than a compliance exercise. Teams are measured by how many vulnerabilities they've remediated, rather than by how effectively they've reduced their organization's exposure.

The siloed nature of cybersecurity, especially between IT and OT teams — each with their own, sometimes contradictory, goals — exacerbates the problem. It is nearly impossible for cybersecurity leaders to obtain a unified and contextual view of their exposure using the existing tools at their disposal. The processes involved — which often require cybersecurity teams to convince their counterparts in IT, cloud and Development Operations (DevOps) to take necessary security precautions

[2] Tenable, "2022 Threat Landscape Report," https://static.tenable.com/marketing/research-reports/Research-Report-2022_Threat_Landscape_Report.pdf
[3] ABC News, "Florida city's water treatment system hacked by 'intruder,' investigators say," https://abcnews.go.com/US/florida-citys-water-treatment-system-hacked-intruder-investigators [4] NPR, "What We Know About The Ransomware Attack On A Critical U.S. Pipeline," https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline
[5] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Shields Up," https://www.cisa.gov/shields-up
[6] Roll Call, "House, Senate members affected in DC Health Link breach to total 21," https://rollcall.com/2023/03/14/house-senate-members-affected-in-dc-health-link-breach-total-21
[7]Ibid 2.

— are fraught with opportunities for error and conflict. The siloed nature of the many preventive security tools offered by cybersecurity vendors means there's no way to determine how much exposure any given weakness actually represents at any given time. The reason? Security pros using siloed tools

are unable to determine the relationships among users, systems and software. Without a unified and contextual view of their environments, security professionals cannot realistically identify the objective security truths that indicate their exposure to risk.

These issues are not new. While applying basic cyber hygiene can reduce exposure, it's long been challenging for organizations to achieve with existing preventive tools. What is new is the expanding complexity of the modern attack surface. Modern IT infrastructure encompasses multiple cloud systems, numerous identity and privilege management tools, multiple web-facing assets along with operational technology (OT) and internet of things (IoT) systems and software.

Today's IT environment brings with it numerous opportunities for misconfigurations and overlooked assets. The lack of a unified and contextual view of users, systems and software means security teams cannot effectively evaluate what's happening across the attack surface. And competing business interests often mean speed and uptime are favored over security.

Government officials and private sector leaders are paying increasing attention to critical infrastructure vulnerabilities, particularly those brought on by the convergence of IT and OT technologies. Since the late 1960s, OT has been part of manufacturing, utilities and other critical infrastructure sectors, and has been considered technology "safe" from attacks because most OT devices were not connected to outside networks. However, in today's modern facilities, these devices are no longer air-gapped and are now in many cases exposed to the internet — and to the threat of cyberattacks.[8]

The combination of IT and OT systems makes OT systems susceptible to the same risks of malware and threats that IT systems face today. Between the two: OT has different performance requirements than IT; OT systems serve a specific purpose while IT systems serve a wide variety of technologies; and OT systems have a lifecycle of a decade or more while IT systems are much shorter. This creates different priorities between IT security professionals and OT system operators within organizations. While IT security practices can inform OT security requirements, the OT systems require more specialized solutions which address the performance requirements of the system.[9]

Securing IT and OT systems and their convergence has become a national security imperative. Public-private sector collaboration to address cyberthreats is essential to building resilient and robust converged IT/OT environments. CISA is the national coordinator for critical infrastructure security and resilience and, as the Administration's National Cybersecurity Strategy emphasizes, it must enhance strategic collaboration and scale public-private partnerships in favor of greater security and resiliency.[10]

Given the heightened threat landscape, CISA and Congress have started to recognize the need to prioritize critical infrastructure security and have begun making much-needed investments. CISA is

[8] Tenable, "Operational Technology (OT) Security: How To Reduce Cyber Risk When IT and OT Converge," https://www.tenable.com/source/operational-technology
[9] President's National Security Telecommunications Advisory Committee, "Information Technology and Operational Technology Convergence Report," https://www.cisa.gov/sites/default/files/publications [10] The White House, "National Cybersecurity Strategy,"
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

working to guide the nation's state and local governments, critical infrastructure providers and other private sector organizations, and federal entities, to strengthen their cyber defenses. In Congress, the House Committee on Homeland Security led efforts to include a $1 billion state and local cybersecurity grant program in the Infrastructure Investment and Jobs Act. The program will help state, local, tribal and territorial governments safeguard these vital systems from future attacks.

CISA 101

CISA was established on November 16, 2018, to defend and secure our nation's cyberspace and build a resilient and robust critical infrastructure for the American people. As a relatively new federal agency, CISA has made strides in elevating cybersecurity and infrastructure security as national security issues. Unlike other well-established federal organizations, CISA is working at start-up speed to keep American organizations ahead of growing and constant cyberthreats.

There has been significant activity under Director Jen Easterly's leadership to strengthen the U.S. cyber posture, including prioritizing public-private partnerships, developing new cybersecurity initiatives and implementing cybersecurity policies proposed by Congress and the Administration.

Joint Cyber Defense Collaborative (JCDC)

CISA established the Joint Cyber Defense Collaborative (JCDC) to lead "integrated public-private sector cyber defense planning, cybersecurity information fusion, and dissemination of cyber defense guidance to reduce risk to critical infrastructure and National Critical Functions."[11] Tenable is a proud Alliance Partner of the JCDC, which has enabled us to collaborate with CISA across a range of cybersecurity issues and challenges, to provide strategic insights and operational response acumen. Managing vulnerabilities is essential to secure critical IT and OT infrastructure and the work done by JCDC and CISA promotes the prioritization of network security. In fact, known vulnerabilities dating as far back as 2017 were so prominent in Tenable's 2022 Threat Assessment Report findings that they occupied the top spot in the 2022 list of the top 5 vulnerabilities.[12]

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Following passage and implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA began development of cyber incident reporting regulations as required by the new law.[13] Timely cyber incident reporting – both from critical infrastructure entities to CISA and from CISA to its industry stakeholders – enables rapid identification, remediation, and proactive defense against these and similar incidents. CISA's commitment to working with industry stakeholders to develop thoughtful, effective, and balanced reporting requirements will further strengthen the cybersecurity of our nation's critical infrastructure.

As part of the regulatory development process, Tenable provided CISA with input as the agency developed its cyber incident reporting regulations required by CIRCIA. Among its input, Tenable proposed the following three primary recommendations to effectively improve threat and incident situational awareness:

[11] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Joint Cyber Defense Collaborative," https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet_508C.pdf [12] Ibid 2.
[13] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),"https://www.cisa.gov/topics/cyber-threats-and-advisories

1. That CISA request contextual details about the specific vulnerability exploited in the cyber incident and actionable information about the nature of the incident, including tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs).
2. That CISA share this information, utilizing the traffic light protocol with a trusted group of cybersecurity stakeholders, such as JCDC Alliance Partners.
3. That actionable information sharing across the critical infrastructure sectors would enable owners and operators to help defend their organizations against and respond to cyberattacks.

Binding Operational Directives (BOD)

CISA also has authority to issue Binding Operational Directives (BOD), which are compulsory directions to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.[14]In 2021, CISA issued BOD 22-01, which requires federal agencies "to remediate vulnerabilities in the KEV catalog within prescribed timeframes."[15] The Known Exploited Vulnerabilities (KEV) catalog is maintained by CISA and helps organizations prioritize remediation of listed vulnerabilities and reduce the opportunities for threat actors to compromise systems.

Following recommendations to conduct asset inventories of OT systems included in last year's NSTAC Report to the President, CISA issued BOD 23-01 to require federal agencies to improve asset visibility and vulnerability detection on federal networks.[16] To provide additional visibility into the variety of assets that make up the modern attack surface and help agencies understand the full scope of their cybersecurity risk, BOD 23-01 mandates continuous and comprehensive asset visibility. The BOD focuses on two core activities that are essential to maintaining a successful cybersecurity program: ● Asset discovery

- Vulnerability enumeration

By mandating continuous and comprehensive asset visibility, BOD 23-01 will ensure that federal agencies have the necessary foundation to maintain a successful cybersecurity program.

This directive applies to all IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols. It builds on BOD 22-01 and outlines new requirements for cloud assets, IPV6 address space, and operational technology (OT) in an effort to reduce cyber risk.

Cross-Sector Cybersecurity Performance Goals (CPGs)

In 2021, the Biden Administration issued the National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems, outlining initiatives in the electricity, pipeline, water, and chemical sectors, and calling for the development of cross-sector cybersecurity performance goals for critical infrastructure.[17]

Last October, CISA released its Cross-Sector Cybersecurity Performance Goals (CPGs), based on relevant categories and subcategories of the NIST Cybersecurity Framework (CSF), to address some of the nation's

[14] 44 U.S.C. § 3552(b)(1). U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Binding Operational Directive 23-01," https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01

[15] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Reducing the Significant Risk of Known Exploited Vulnerabilities," https://www.cisa.gov/known-exploited-vulnerabilities

[16] Ibid 9.

[17] The White House, "National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems," https://www.whitehouse.gov/briefing-room/statements-releases

most frequent and impactful cybersecurity risks. The CPGs also emphasize OT security and how it is often overlooked and under-resourced.[18] By offering IT/OT cybersecurity guidance, CISA's CPGs create a baseline set of cybersecurity practices and benchmarks for critical infrastructure operators to measure and improve their cyber posture. Earlier this week, CISA released stakeholder-based updates to the CPGs that are more strongly aligned with the functions, categories, and subcategories of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is widely utilized by critical infrastructure owners and operators and the greater alignment of the CPGs will make them more accessible to these entities.

Pillar One of the Administration's new National Cybersecurity Strategy builds on this notion of

establishing cybersecurity best practices and expanding the use of minimum cybersecurity standards, such as the adoption of basic cyber hygiene and secure-by-design principles. This reinforces that IT/OT convergence will continue to be a security issue for years to come, and organizations need a plan to address these challenges.[19]

Tenable was pleased that CISA incorporated input from multiple critical infrastructure industry stakeholders, including relevant sector coordinating councils (SCCs) in the development of the CPGs, ensuring they were aligned with the NIST CSF. We are also encouraged to see the Administration emphasize similar approaches to mitigate cybersecurity risk in its National Cybersecurity Strategy. Baseline cybersecurity requirements or standards of care for critical infrastructure, which align with CISA's Cross-Sector Cybersecurity Performance Goals, international standards, and the NIST CSF, drive better cybersecurity and a more resilient ecosystem.

Secure-by-Default

In recent months, CISA has spearheaded efforts to shift the security burden from consumers to putting the onus on manufacturers to ensure built-in security is a feature of all technology products, especially those that support critical infrastructure. Director Easterly stated, "the leaders of technology manufacturers should explicitly focus on building safe products, publishing a roadmap that lays out the company's plan for how products will be developed and updated to be both secure-by-design and secure-by-default."[20] Likewise, CISA launched the Ransomware Vulnerability Warning Pilot program to help identify vulnerabilities in critical infrastructure systems and inform owners to take action before a potential cybersecurity incident occurs.[21]In conjunction with the other initiatives CISA has developed, these efforts will work to advance the nation's cybersecurity resiliency.

Separation of Duties / Independent Assessments of Software

Similar to the Sarbanes-Oxley Act of 2002 requirement for firms to separate their auditing function from their consulting function, "separation of duties" in cybersecurity is necessary to prevent conflicts of interest, misaligned incentives, and increased security risks. The U.S. Securities and Exchange Commission states that an auditor is not capable of exercising objective and impartial judgment if a

[18] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[19] The White House, "National Cybersecurity Strategy," https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [20] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "The Cost of Unsafe Technology and What We Can Do About It," https://www.cisa.gov/news-events/news/cost-unsafe-technology-and-what-we-can-do-about-it [21] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "CISA Announces Ransomware Vulnerability Warning Pilot," https://www.cisa.gov/news-events/alerts/2023/03/13

relationship with or service provided by an auditor "(a) creates a mutual or conflicting interest with their audit client; (b) places them in the position of auditing their own work…"[22]

CISA should apply the Sarbanes-Oxley "separation of duties" principles to cybersecurity and prohibit the provider responsible for developing and/or running software programs from also testing its security, conducting security audits, or reporting on its security.

What's Next: CISA 2025

CISA has worked to enable organizations and critical infrastructure providers to understand, manage, and reduce their cybersecurity risks, but there is still much work to be done. Naturally, as the agency evolves, there is a significant need for continued improvements to strengthen our cybersecurity efforts and to address the many unique needs of the critical infrastructure sectors.

While some of the 16 identified critical infrastructure sectors[23] have a high degree of cybersecurity preparedness, strong risk understanding and risk management practices, and very strong security programs, others are woefully ill prepared. New technology investments represent great efficiency opportunities, like the move to smart factories and smart cities, but these shifts can introduce real gaps in security. Continued digital transformation, increasingly interconnected IT and OT systems, and an expanding cyberattack surface will require enhancements to security and resiliency. Critical infrastructure providers must be prepared to address tomorrow's cyberthreats and it is CISA's responsibility to support them in that effort.

Zero Trust Architecture

The White House issued a Federal Zero Trust Architecture (ZTA) Strategy in January of 2022, requiring agencies to implement Attack Surface Management (ASM) as part of their ZTA by the end of fiscal year 2024. The memorandum states, "to effectively implement a zero trust architecture, an organization must have a complete understanding of its internet-accessible assets so that it may apply security policies consistently and fully define and accommodate user workflows."[24] ASM enables organizations to identify assets and look for vulnerabilities from the outside in, from the attacker's perspective, and will give agencies complete asset discovery, increase awareness of what is on their networks, and improve vulnerability management.

The memorandum further states, "for agencies to maintain a complete understanding of what internet-accessible attack surface they have, they must rely not only on their internal records, but also on external scans of their infrastructure from the internet."[25] Ultimately, organizations cannot take a 'trust no one' approach on a device if they do not know the device exists; however, ASM enables that visibility.

As agencies look to comply with the White House's ZTA strategy by moving towards a zero trust architecture and taking a 'trust no one' approach to security, the security of an agency's underlying user identity and privilege management system itself comes into play. To ensure identity systems are secure, agencies need to be able to identify everything in their complex Active Directory (AD) environment,

[22] The U.S. Securities and Exchange Commission, "Audit Committees and Auditor Independence," https://www.sec.gov/oca/audit042707
[23] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[24] The White House, "Federal Zero Trust Architecture (ZTA) Strategy," https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[25] Ibid 24.

predict what matters to reduce risk, and eliminate attack paths before attackers exploit them. Effective management of AD users and privileges allows agencies to take a proactive approach to address and mitigate future cyberthreats.

NSTAC IT/OT Convergence Report

In response to growing cybersecurity threats to the critical infrastructure upon which Americans depend, the White House tasked The President's National Security Telecommunications Advisory Committee (NSTAC) with conducting a multi-phase study on "Enhancing Internet Resilience in 2021 and Beyond."[26] The Subcommittee for the second phase of the study was charged with developing the NSTAC Report to the President on IT/OT Convergence.[27]I co-led the subcommittee's working group to produce this report. The report identifies three opportunities for the federal government:

- to help relevant stakeholder communities execute a secure convergence of IT and OT cybersecurity;

- to examine the key challenges of securing converged OT systems against threats that emerge from IT network connections; and
- to identify emerging approaches to increase OT resiliency to these threats

The subcommittee received briefings from more than 30 subject matter experts across government and private industry. First, the subcommittee heard from government owners and operators of OT systems and policymakers focused on IT and OT cybersecurity; second, we heard from critical infrastructure owners and operators of converged IT/OT environments and original equipment manufacturers; and third, we heard from cloud service providers, integrators, and cybersecurity vendors.

NSTAC Report Findings

On August 23, 2022, NSTAC approved the Report to the President. The report findings revealed several consistent themes highlighting that the convergence of IT and OT systems is not a new issue. As a nation, we have not prioritized securing IT/OT interconnected systems, despite having the technology and knowledge readily available. Even in 2022, the report found organizations lack visibility into their OT environments, which is exacerbated by the traditional silos within which OT and IT personnel operate. The current siloed approach demonstrates a need to promote harmonization through a unified structure to better manage shared responsibility to secure converged environments.[28]

Stakeholders also rarely take the opportunity to proactively "build in" security where appropriate and opt instead to "bolt-on" security in OT environments after the fact, costing organizations valuable time and resources to recover from cyber incidents and unpatched vulnerabilities.

Businesses, organizations, and governments need to share the responsibility of building a more sustainable cybersecurity model to create ecosystems that take a secure-by-design approach to ensure the long-term cybersecurity resiliency of our country - a point Director Easterly and CISA Executive Director Eric Goldstein recently emphasized.[29]

[26] President's National Security Telecommunications Advisory Committee, "NSTAC Fact Sheet,"https://www.cisa.gov/resources-tools/resources/presidents-nstac-fact-sheet
[27] Ibid 9.
[28] Ibid 9.
[29] Foreign Affairs, "Stop Passing the Buck on Cybersecurity,"
https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity

NSTAC Recommendations to Improve Critical Infrastructure Security

Based on the findings, the subcommittee developed 15 presidential, strategic, and actionable recommendations to address the many concerns expressed to the subcommittee through the briefing phases. Amongst the 15 recommendations, the subcommittee identified three consequential recommendations for the President to strengthen the cybersecurity posture of U.S. government owned and operated OT systems that should be prioritized.

The report first recommends that CISA issue a Binding Operational Directive (BOD), similar to what Section 1505 of the Fiscal Year 2022 National Defense Authorization Act (NDAA) requires for the Department of Defense (DoD), that requires executive civilian branch departments and agencies to maintain a real-time, continuous inventory of all OT devices, software, systems, and assets within their areas of responsibility, including an understanding of any interconnectivity to other systems. An up-to-date inventory should be required as part of each department's or agency's annual budget process.

Once federal agencies clearly understand the vast and interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions about how to prioritize their cybersecurity budgets to best protect the most consequential of those assets.

Second, CISA should develop guidance on procurement language for OT products and services, and for products and services that support converged IT/OT environments, to incentivize the inclusion of risk-informed cybersecurity capabilities, including for supply chain risk management. This guidance should also help organizations understand best practices for bolt-on security for legacy OT devices that are difficult or expensive to replace.

CISA should work with the General Services Administration (GSA) to require the inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the federal government. There should also be a mechanism for both private sector users of the procurement guidance and public sector agencies, which must follow the new requirements, to provide feedback and lessons learned to aid the community.

Finally, the NSC, CISA, and the Office of the National Cybersecurity Director (ONCD) should prioritize developing and implementing interoperable, technology-neutral, vendor-agnostic information-sharing mechanisms to enable real-time sharing of sensitive collective-defense information between authorized stakeholders involved with securing U.S. critical infrastructure. This should include breaking down the artificial barriers for sharing controlled unclassified information, both within the U.S. government and between government and other key, cross-sector stakeholders.

Additional recommendations in the report to secure U.S. OT infrastructure call on CISA and the ONCD to clearly articulate roles and responsibilities for federal agencies that support critical infrastructure and other industry stakeholders. Concurrently, CISA should work with the Office of Management and Budget (OMB) to develop key IT/OT convergence cybersecurity performance indicators and implementation timelines for agencies and hold agency heads accountable. Furthermore, the ONCD, in partnership with CISA, should facilitate an interagency study that evaluates conflicting regulations for OT operators to identify opportunities to streamline OT cybersecurity regulation.

Based on the subcommittee briefings, it was evident that the federal government has historically underfunded OT cybersecurity. Fortunately, the Infrastructure Investment and Jobs Act (IIJA) has created

numerous grant programs that include cybersecurity as an allowable expense, presenting an opportunity for the ONCD and CISA to collaborate with Sector Risk Management Agencies (SRMA) to ensure that cybersecurity is a priority item in any grant application. Of note, the State and Local Cybersecurity Grant Program (SLGCP) appropriates $1 billion in grant funding over the next four years to help advance OT cybersecurity. Tenable has been leading efforts to educate eligible entities on how to apply for grant funding and implement cybersecurity solutions that address the growing threats and risks to their information systems.[30]

Binding Operational Directive 23-01

As previously mentioned, last October CISA issued Binding Operational Directive (BOD) 23-01, calling on federal civilian departments and agencies to “make measurable progress toward enhancing visibility into agency assets and vulnerabilities,” aligning with NSTAC’s IT/OT Convergence Report recommendations.[31]

BOD 23-01 mandates continuous and comprehensive asset visibility, focusing on two core activities essential to maintaining a successful cybersecurity program: asset discovery and vulnerability enumeration. According to BOD 23-01, "continuous and comprehensive asset visibility is a basic

precondition for any organization to effectively manage cybersecurity risk. Accurate and up-to-date accounting of assets residing on federal networks is also critical for CISA to effectively manage cybersecurity for the Federal Civilian Executive Branch (FCEB) enterprise."[32] Federal agencies need comprehensive visibility into their assets and vulnerabilities across their organizations to protect against external unknowns.

Enumerating OT assets, critical infrastructure and vulnerabilities present unique challenges to federal agencies. Compared to the IT environment, where patching, upgrading and replacing systems is standard, an OT environment typically requires working with legacy technologies. To prioritize remediation efforts, agencies need a detailed view of OT and IT assets in the OT environment and the ability to map connections between devices and identify high-risk assets.

To ensure FCEB systems and agencies operating those systems meet said requirements, Congress should appropriate funding to implement CISA's BOD 23-01, enabling agencies to maintain an updated inventory of assets, identify software vulnerabilities, track how often an agency enumerates its assets, and share information with CISA's Continuous Diagnostics and Mitigation Program (CDM) Federal Dashboard. Pursuant to BOD 23-01, the scope of this implementation encompasses all reportable OT as well as IT assets.

Policy Recommendations

Congressional action should not allow for "learned helplessness" by federal government agencies or private industry. There is too much at stake for individuals and organizations to remain negligent and not take even the most basic steps to improve their cyber posture..

Tenable recommends the following steps that Congress should implement to enhance the cyber preparedness of U.S. critical infrastructure:

[30] H.R.3684 – 117th Congress (2021-2022): Infrastructure Investment and Jobs Act. (2021, June 4). https://www.congress.gov/bill/117th-congress/house-bill/3684/text
[31] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Binding Operational Directive 23-01," https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01 [32] Ibid 31.

- **Establish baseline cybersecurity requirements or standards of care for critical infrastructure that align with CISA's Cross-Sector Cybersecurity Performance Goals, international standards, and the NIST CSF, based on effective cyber hygiene and preventive security practices.** Basic cyber hygiene for critical infrastructure operators includes continuous understanding of what assets are on networks, ensuring strong identity and access management, scanning for and patching known vulnerabilities, and implementing incident detection and response capabilities. Pillar One of the recently released National Cybersecurity Strategy calls for baseline cybersecurity requirements for critical infrastructure providers. The CISA Cross-Sector Cybersecurity Performance Goals, based on the NIST CSF, are an excellent resource for industry and Sector Risk Management Agencies to utilize in the development of baseline requirements and standards of care.

- **In its oversight of CISA implementation of CIRCIA, Congress should ensure that CISA:** is adequately resourced to ingest the wealth of information that will be shared by critical infrastructure entities; will request and share anonymized data on the types of vulnerabilities that were exploited and the attack paths that adversaries followed after infiltrating target networks; and provides actionable information through trusted partners, such as JCDC Alliance Partners, to provide cyber situational awareness to the broader critical infrastructure ecosystem to enable entities to protect themselves against ongoing and potential attacks.

- **Require Independent Assessments of IT Management Software.** CISA should apply the Sarbanes-Oxley "separation of duties" principles to cybersecurity and prohibit the provider responsible for developing and/or running IT management software from also conducting its exposure management or otherwise testing its security, conducting security audits, or reporting on its security.

- **Continue implementation of the NSTAC IT/OT Convergence Report policy recommendations**. o **Direct federal civilian agencies to inventory their OT assets and provide OT asset and vulnerability information to the CDM Dashboard.** CISA has already taken steps to address this obstacle through BOD 23-01, but Congress should reinforce the need to gain visibility into these mission-critical environments so we can understand the scale of cybersecurity challenges and begin to systematically address the serious risk. The foundation for every security framework, whether IT or OT, always begins with visibility into the assets for which you are responsible. Achieving this visibility is a significant step forward for federal departments and agencies to protect their critical IT and OT assets against evolving cybersecurity threats.
  - o **Develop enhanced OT-specific cybersecurity procurement language.** Public and private sector OT requests for proposals and procurement processes seldom require the inclusion of risk-informed cybersecurity capabilities for products and services. Updating procurement language guidance will help asset owners specify that cybersecurity be built into products and projects rather than bolted on as an afterthought. Including cybersecurity in both government and private sector procurement vehicles will significantly enhance the resilience of critical infrastructure systems.
  - o **Implement standardized, technology-neutral, real-time interoperable information sharing mechanisms** to promote the sharing of sensitive information across agencies and to break the traditional siloed approach. Cyberattacks often target multiple critical infrastructure sectors and attackers have the ability to move at machine speed to

compromise multiple industrial sectors. Our defenses need to match this threat and it is imperative for our critical infrastructure sectors to securely communicate with each other to get the right information to the right person, at the right time, in a standardized, technology-neutral way, in order to leverage cyberthreat and vulnerability information from the broader critical infrastructure ecosystem.

- **Ensure CISA and FCEB agencies are adequately resourced to implement BOD 22-01 and BOD 23-01 policy recommendations.** Protecting our nation's cybersecurity means knowing what's on our networks and maintaining it in good working order, which includes conducting an inventory of OT assets and prioritizing remediation of known vulnerabilities. If an organization does not know an asset exists, it cannot scan it for vulnerabilities. With the issuance of BOD 23-01, federal agencies need comprehensive visibility into their assets and vulnerabilities across their organization. This includes:
  - o External unknowns
  - o Cloud workload and resources
  - o Operational technology
  - o Network infrastructure and endpoints
  - o Web application
  - o Identity systems

- **Ensure sufficient funding for CISA and the Office of the National Cyber Director to ensure they can meet mission requirements.** Our company supported the creation of the Office of the

National Cyber Director and applauded efforts to stand up and staff the new office. The threats to federal networks and critical infrastructure are growing at a significant rate, and CISA must serve as an effective coordinator to strengthen security in these environments. Congress should see the FY 2024 appropriations for CISA as a new baseline number, which should grow at a rate commensurate with the needs of the mission.

- **Support and strengthen value added engagement between the private sector and public sector**. The JCDC, of which Tenable is a member, is bringing together representatives from private industry and key government agencies to drive strategic planning and incident response capabilities. This type of operational government-industry engagement has been a positive step forward and we urge Congress to continue supporting and strengthening the JCDC's alignment.

- **Accelerate deployment of Zero Trust including Active Directory and Attack Surface Management.** Congress should provide federal agencies with the resources needed to implement Cyber Executive Order 14028 to modernize and strengthen our collective cyber defenses, recognizing that Zero Trust is a philosophy that dictates systems design and operation, not a singular product.
    - o **All government systems must incorporate Active Directory security** to ensure least privileges for user identities, and to scan for misconfigurations that can be exploited to gain access to Active Directory and monitor for ongoing suspicious and high-risk activities within Active Directory.[33]
    - o **Attack Surface Management,** which continuously scans the internet to discover, inventory, classify, and monitor an organization's IT infrastructure, **will give agencies**

[33] U.S Department of Commerce, "NOAA Inadequately Managed Its Active Directories That Support Critical Missions," https://www.oig.doc.gov/OIGPublications/OIG-22-018-A.pdf

complete asset discovery, increase awareness of what is actually on their networks, and will improve vulnerability management.

<u>Conclusion</u>

There are fundamental steps all federal agencies and critical infrastructure sectors must take — from knowing what's on their network and how those systems are vulnerable to addressing known exposures, and from controlling user access and privileges to managing critical systems that are interconnected — that will make it harder for bad actors to compromise interconnected IT and OT systems.

Many critical operating environments lack a formal systemic approach to risk assessments and processes, let alone the continuous visibility expected for critical services and high value targets. These formal processes are desperately needed as rapid increases in access and interconnectivity dramatically increase risk**.** In these instances, policy guidance for transparency and standards of care can help drive improvements in risk management practices and at the same time foster innovation.

Thank you Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and members of the Subcommittee for your attention to these important issues and continued assessment of the work CISA is doing to keep Americans safe. I appreciate the work this committee is doing to elevate cybersecurity with bipartisan support. Thank you for the opportunity to testify today and I look forward to working with you to secure our nation's cyber assets.